

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
3 July 2003 (03.07.2003)

PCT

(10) International Publication Number  
**WO 03/055261 A1**

(51) International Patent Classification<sup>7</sup>: **H04Q 7/38**

(21) International Application Number: **PCT/SE02/02379**

(22) International Filing Date:  
18 December 2002 (18.12.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
0104325-6 20 December 2001 (20.12.2001) SE

(71) Applicant (for all designated States except US): **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)**  
[SE/SE]; S-126 25 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **SUNDBERG,**  
Per-Erik [SE/SE]; Svalvägen 4, S-187 43 Täby (SE).

(74) Agent: **BERGENSTRÅHLE & LINDVALL AB**; Box  
17704, S-118 93 Stockholm (SE).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

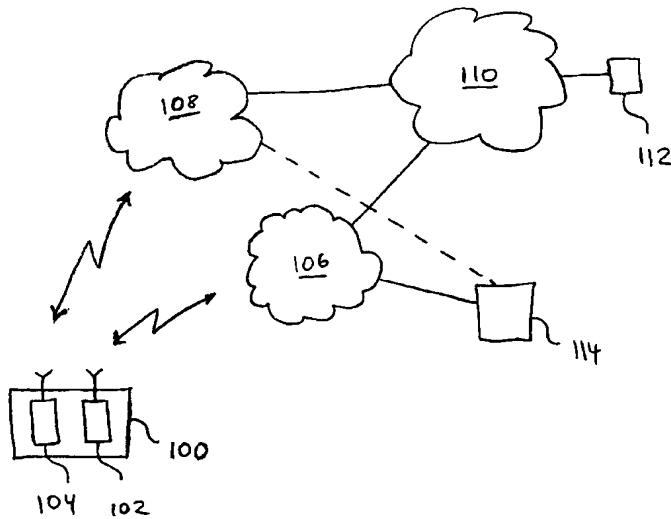
— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A METHOD AND APPARATUS FOR SWITCHING ACCESS BETWEEN MOBILE NETWORKS



**WO 03/055261 A1**



(57) Abstract: A method and apparatus for switching access between mobile networks for a mobile terminal (100) comprising a first and a second radio device (102, 104) capable of communication with a first and a second mobile network (106, 108), respectively. The second mobile network (108) has priority over the first mobile network (106). A first connection is authorised and established between the first radio device (102) and the first mobile network (106). When it is detected that the mobile terminal (100) moves into a coverage area of the second mobile network (108), a second connection is authorised and established between the second radio device (104) and the second mobile network (108) based on the authorising made for the first connection with the first mobile network (106). Both connections can then rely on the authorisation of the first connection.

A METHOD AND APPARATUS FOR SWITCHING ACCESS BETWEEN MOBILE NETWORKS

TECHNICAL FIELD

5       The present invention relates generally to a method and apparatus for switching access for a mobile terminal between overlapping mobile networks. In particular, the handover procedure between mobile networks is facilitated.

10

BACKGROUND OF THE INVENTION AND PRIOR ART

Mobile access networks are often designed as cellular networks including a plurality of base stations being connected together by means of switching nodes such as  
15 Base Station Controllers (BSCs) and/or Mobile Switching Centres (MSCs). Each base station provides radio coverage over an area known as a cell, for communication over radio channels with mobile terminals located in the cell. When a communicating mobile terminal moves across a cell border,  
20 its radio connection switches between the corresponding base stations by means of a "handover" or "handoff" procedure. Each mobile network operator is allocated a certain limited radio frequency spectrum for transmissions, and efforts are made by network designers to provide a high traffic capacity  
25 within the allocated spectrum.

When setting up radio connections with mobile terminals, standardised communication protocols and radio channels are used, such as those defined for GSM, TDMA, PDC, UMTS, etc, for transmission of speech and/or data over the  
30 air interface as well as within the network, providing a certain data rate. Digital circuit switched radio channels of today, e.g., according to the GSM standard, are primarily

designed for communication of encoded speech, providing data rates of less than 10 kbit/s.

Existing GSM networks are currently being extended with packet based GPRS (General Packet Radio Service)

5 technology, providing packet switched radio communication with enhanced data rates ranging between 10 and 120 kbit/s for mobile terminals having GPRS capabilities. Further switching nodes, such as Gateway GPRS Service Nodes (GGSNs) and Serving GPRS Service Nodes (SGSNs), are included in GPRS  
10 networks. GSM/GPRS networks and other cellular networks typically provide radio coverage over large areas, often covering entire countries, more or less.

Currently, enhanced wireless access technologies are emerging having far greater data rates, such as WLAN (Wireless Local Area Network), covering much smaller areas and providing so-called "spot coverage" over distances around 100 meters. WLAN stands for a plurality of high-speed wireless technologies, e.g., employing frequency hopping and spread-spectrum radio technologies not further discussed  
20 here, for packet based radio communication with data rates ranging between approximately 2 – 54 Mbit/s. Radio channels are used in freely available frequency bands, such as 2,4 GHz and beyond, requiring no operator licence.

A WLAN may use one or more radio stations as access points to which mobile terminals having WLAN capabilities may be connected over predefined radio channels. A WLAN radio station may be directly connected to a extension of a fixed LAN (Local Area Network) which in turn, through various gateways and/or routers, may provide access to the  
30 global Internet or to a company intranet. In the case of Internet, a service is normally utilised from a public telecommunication operator.

WLAN typically provides a limited spot coverage geographically overlapping the larger coverage of cellular networks, such as GSM/GPRS networks. The cellular networks can offer connectivity in urban areas as well as in rural areas, whereas WLAN can offer high speed connections in small hot spot areas. WLAN for public access is currently used mainly in airports, hotels and conference venues, providing fast Internet access and other data services to visitors.

Today, work is in progress for developing a multitude of new mobile services, which will be possible to employ in particular as new technologies with greater capacity and higher data rates are introduced. The contents of the new services include voice, text, images, audio files and video files in various different formats and combinations. Internet browsing is also becoming very popular, and in recent years, the wireless and Internet domains are converging.

More sophisticated mobile terminals are also becoming available on the market, provided with functionality matching the new services. Furthermore, it is possible to combine different mobile terminals. For example, a portable laptop computer may be connected to a mobile phone by means of a cable or a wireless interface, such as a Bluetooth radio interface. The mobile phone can then be used as a radio unit providing access over a cellular network, such as a GSM/GPRS network, and the laptop is utilised as an enhanced user interface, whereas the mobile phone acts as a "modem". Laptop computers may also be provided with a radio device, e.g., implemented as a PCCARD or the like, for radio access to a WLAN. Alternatively, plural radio devices may be integrated in a single terminal, e.g., a laptop computer,

for radio communication with different networks, such as a WLAN and a GSM/GPRS network.

For users having a mobile terminal equipment capable of radio communication over multiple access networks, either as a single integrated device or as plural interconnected devices, it is desirable that the mobile terminal is automatically connected to the access network providing the highest data rates, if more than one network is currently available. The user will then benefit from the best available communication possibilities in any given location. For example, a user having a laptop with WLAN capabilities interconnected with a mobile phone with GSM/GPRS capabilities, will want to switch access to a WLAN when entering its coverage area, instead of being connected to the more limited GSM/GPRS network.

In applicant's own PCT application WO 01/35585, it is described a mechanism for selecting the "best" and optimal network connection, when more than one network is available to one or more end devices. The selection is made with respect to factors such as available bandwidth, charge rate, quality, individual preferences, etc.

An access switch between two networks requires that a new radio connection is established with the new network, involving the creation of a new communication session context. The present invention aims at facilitating the switching of access between different networks with maintained security.

Creating a communication session context includes performing certain pre-defined routines for authentication, authorisation and accounting, sometimes referred to as AAA for short. Cellular networks employ AAA routines according to their standardised communication protocols, which are

regarded as having a fairly high level of security. For example, each mobile phone may be provided with a secret identity code or the like which is known in the network and is used for authentication and/or for generating encryption keys. The identity code may be stored in a smart card, such as a SIM (Subscriber Identity Module) card as used in GSM, which is movable between different terminals.

A WLAN connection may be secured by means of a certificate stored in the terminal, which is regarded as trustworthy and is used to verify the identity of the user or subscriber. The certificate may also be used for generating various encryption keys and/or session keys to authenticate the terminal and to protect an ongoing session according to well-known techniques, which will not be described here further. The certificate may be issued by a certification authority and may comprise one or more secret codes. However, such secret codes, certificates and encryption keys are cumbersome to administrate and distribute, in particular to subscribers of the general public.

In addition to using stored codes and certificates in the terminal, some services, e.g., Internet services, require a login procedure involving a shared secret, normally a user ID/password combination.

In present solutions, when a mobile terminal with multiple capabilities switches from a first network to a second network, it is a problem that the session context of the first connection is lost and a new session context must be established with the second network, involving a new authentication procedure, among other things. This is the case when, for example, switching between a GSM/GPRS network and a WLAN in either direction. The new session context may

further determine different user interface features, available services and charge rates, as dictated by the second network.

Establishing a session context is a fairly complex procedure, and if two different networks are to be accessed, two separate authentication mechanisms having a certain level of security are required, each involving the distribution and storing of secret codes and/or certificates. Further, both networks need one or more nodes with protected links for performing authentication routines.

It is desirable to reduce the handling of shared secrets between a subscriber and network operators, at the same time maintaining security. It is also desirable that the amount of exchanged information and processing work are minimised when switching between networks for reducing the load on transmission resources and to reduce delays.

#### SUMMARY OF THE INVENTION

The object of this invention is to reduce or eliminate the problems outlined above. This object and others are obtained by providing a method and apparatus for switching access for a mobile terminal between mobile networks. The mobile terminal comprises a first radio device capable of communication with a first mobile network and a second radio device capable of communication with a second mobile network. The second mobile network has priority over the first mobile network, for example by offering a higher transmission bitrate, a higher quality and/or enhanced services.

According to the inventive method, an access request is made to the first mobile network by the mobile terminal using the first radio device. A first connection is

authorised and established between the first radio device and the first mobile network. Payload data may then be communicated over the first connection with the limited bitrate/quality/services as offered by the first mobile  
5 network. Later, it is detected that the mobile terminal moves into a coverage area of the second mobile network. A second connection is then authorised and established between the second radio device and the second mobile network based on the authorising made for the first connection with the  
10 first mobile network.

When authorising the second connection, authentication information is exchanged between the first radio device and an authentication unit in the first mobile network, which authentication information is used by the  
15 second radio device for accessing the second mobile network. In this way, authorisation of the second connection relies on the authorisation made for the first connection, thereby substantially facilitating the access switch from the first to the second network. The security level of the first  
20 network is also maintained and utilised for the second mobile network.

The exchanged authentication information may comprise login information and one or more encryption keys, according to a predetermined authentication agreement  
25 between the first and second mobile networks. Payload data communicated between the second radio device and the second mobile network in the second connection may then be protected by the one or more exchanged encryption keys.

The present invention further embraces a mobile  
30 terminal comprising a first radio device capable of communication with a first mobile network and a second radio device capable of communication with a second mobile

network, wherein the second mobile network has priority over the first mobile network. The first radio device includes means for making an access request to the first mobile network and means for authorising and establishing a first connection between the first radio device and the first mobile network. The first radio device further includes means for authorising a second connection between the second radio device and the second mobile network based on the first authorised connection with the first mobile network,

5 when it is detected that the mobile terminal moves into a coverage area of the second mobile network.

10

The present invention further embraces an authentication unit for authenticating a mobile terminal comprising a first radio device capable of communication with a first mobile network and a second radio device capable of communication with a second mobile network, wherein the second mobile network has priority over the first mobile network. The authentication unit includes means for authorising and establishing a first connection between the first radio device and the first mobile network in response to an access request from the first radio device.

15

The authentication unit further includes means for exchanging authentication information with the first radio device when it is detected that the mobile terminal moves into a coverage area of the second mobile network, wherein the exchanged authentication information is used by the second radio device for accessing the second mobile network.

20

25

#### BRIEF DESCRIPTION OF THE DRAWINGS

30 The present invention will now be described in more detail and with reference to the accompanying drawings, in which:

- Fig. 1 is a schematic view of a communication scenario in which the invention may be implemented.
- Fig. 2 is a schematic signalling diagram of a procedure for switching between two networks.

5

#### DESCRIPTION OF PREFERRED EMBODIMENTS

Fig. 1 is a schematic view of an exemplary communication scenario in which the present invention may be implemented. 100 denotes a mobile terminal equipment generally comprising a first radio device 102 and a second radio device 104 for communication with first and second mobile access networks 106 and 108, respectively. By way of example, the first radio device 102 may be a mobile phone for radio communication with a cellular network 106, and the second radio device 104 may be a laptop computer equipped with a PCCARD or the like for radio communication with a WLAN 108. The mobile phone 102 and the laptop 104 are interconnected by means of a communication link, such as a cable, a Bluetooth interface or an infrared link. The functionality of both the mobile phone 102 and the laptop 104 may therefore be used, regardless of which network is connected.

It should be understood that the mobile terminal 100 is only logically represented in Fig. 1 as two radio devices 102, 104, but can be designed in many alternative ways within the scope of the present invention. For example, the mobile terminal 100 may instead be one integrated unit, such as a single laptop with a PCCARD or a single mobile phone, either being capable of radio communication with both networks 106 and 108.

Both networks 106, 108 are further connected to a backbone network 110, which may be the Internet, an

intranet, a fixed public or private network, or any combination of such networks. A server 112 is connected to the backbone network 110, providing service to the mobile terminal 100 in this case.

5       The first network 106 covers a wide geographic area, and the second network 108 covers a limited overlapping spot area, and can provide a higher data transmission rate than the first network 106. It is therefore preferred that the mobile terminal 100 is  
10      connected to the second network 108 when being within the spot coverage area of the second network 108. The second network 108 may also provide a higher quality or enhanced services. Generally speaking, the second network 108 has priority over the first network 106.

15      The first network 106 comprises an authentication unit 114 having access to various authentication information which is used for authenticating the mobile terminal 100. The authentication information is stored in a database, such as a HLR (Home Location Register), not shown, and may  
20      include identity codes and/or certificates matching similar information stored in the terminal or in a SIM card or the like inserted therein.

An exemplary procedure will now be described for accessing the first network 106 and then switching access to  
25      the second network 108, with reference to a signalling diagram in Fig. 2. Corresponding elements are denoted with the same reference numbers as in Fig. 1.

Firstly, the mobile terminal 100 makes access to the first network 106 using the first radio device 102, in a  
30      first step 200. When setting up the connection, a session context is established, including an authentication procedure. The session context may further include setting

parameters such as user interface features, service features, a charge rate and communication protocols, including a data rate.

- The authentication procedure involves exchanging  
5 of secret codes and/or certificates between the mobile terminal 100 and the authentication unit 114, in a step 202, according to a routine which is predefined in the first network 106. For example, if the first network 106 is a GSM/GPRS network, a SIM card in a mobile phone is used.  
10 Different network types have their own specific predefined authentication procedures as dictated by standardised protocols, which will not be described here further.

When the session context is created and a connection is authorised, the mobile terminal 100 may begin  
15 to communicate payload data over the first network 106, in this case with a server 112 providing service to the mobile terminal 100, in a step 204. The data rate is then limited to the bitrate offered by the first network 106. Since the two radio devices 102, 104 are interconnected, the  
20 functionality and user interface of both may be used by a user, as described above. For example, an IP (Internet Protocol) connection may be established between a mobile phone 102 and a packet core network, not shown, in the first network 106, which IP connection may be available to a  
25 laptop computer connected to the mobile phone 102.

If the mobile terminal 100 moves into the coverage area of the second access network 108, this can be detected automatically in a step 206, preferably by means of the second radio device 104. The presence of the mobile terminal  
30 100 in the coverage area of the second network 108 can in fact be detected in different ways. Three exemplary alternatives are given below:

1. The second network 108 transmits an identification signal which the mobile terminal 100 can detect in the second radio device 104, such as a PCCARD or the like installed in a laptop computer. For example, in a WLAN, access points continuously transmit an identifier, typically named ESSID (Extended Service Set Identifier) and/or SSID, which the second radio device 104 can receive and recognise as identifying the WLAN.  
5
2. The second radio device 104 transmits an identification signal which is detected by the second network 108, which then may notify the radio device 104 accordingly.  
10
3. A locating function determines that the mobile device 100 is located within the second network 108. The locating may be performed by a GPS (Global Location System) unit, or by a function in the first network 106, such as triangulation. Such locating functions are currently used for, e.g., transmitting location dependent messages to mobile terminals and for searching purposes. The GPS unit or the first network 106 may then notify the mobile  
15
- 20

When the availability of the second network 108 to the mobile terminal 100 has been detected, as described in step 206, a new connection with the second network 108 is authorised, based on the authorising for the connection with the first network 106 made in step 202. The first radio unit 102 and the authentication unit 114 then exchanges information, in a step 208, for authorising and establishing the new connection with the second network 108.

The first radio unit 102 may begin by sending an access request. The authentication unit 114 then replies by sending login information, such as a login identity and a temporary password, which the mobile terminal 100 can use

when accessing the second network 108 by means of the second radio unit 104. The authentication unit 114 may also send one or more encryption keys to be used during the login procedure and/or during the communication session. The first 5 network 106 has a predetermined authentication agreement with the second network 108, valid for the mobile terminal 100, including the exchanged login information and encryption keys, which are thus already known in the second network 108.

10 The second network 108 and the second radio unit 104 then exchanges various messages for establishing a new session context, in a step 210, using the login information and encryption keys obtained in step 208.

15 In this way, the authentication done with the first network 106 in step 202 is utilised for authorising the new session with the second network 108 in step 210. For example, the second network 108 may comprise a subscriber administration server having the agreed login information and encryption keys stored therein. The subscriber 20 administration server of the second network 108 may be integrated with the authentication unit 114 of the first network 106 in one server common to both networks 106, 108.

25 Hence, the high level of security offered in the first network 106 is utilised by the second network without requiring its own administration and distribution of secret codes and certificates. The authentication procedure in step 210 is also facilitated by reducing the amount of exchanged information, thereby also reducing delays and transmission load.

30 When the new session context is established and a connection with the second network 108 is authorised, the mobile terminal 100 may communicate payload data with the

server 112 by means of the second radio device 104, in a step 212. In this case, the data rate is then increased to the higher bitrate offered by the second network 106. Further, the communicated payload data may be protected by 5 encryption keys issued by the authentication unit 114 of the first network 106 during step 208. The access switch over to the second network 108 is fully automatic, requiring no efforts from a user.

If the mobile terminal 100 moves out of radio 10 coverage of the second network 108, the connection breaks down in a step 214, and the session automatically reverts to the first network 106 by means of the first radio device 102, in a step 216. Since this connection was already authorised in step 202, no further authentication actions 15 are required.

In practice, the invention may be implemented in a computer program for use in the mobile terminal 100, and in a computer program for use in the authentication unit 114.

By using the described invention, access switching 20 between two networks is facilitated with maintained security, without requiring manual efforts from a user. Also, delays and transmission load are reduced.

While the invention has been described with reference to specific exemplary embodiments, the description 25 is only intended to illustrate the inventive concept and should not be taken as limiting the scope of the invention. Various alternatives, modifications and equivalents may be used without departing from the spirit of the invention, which is defined by the appended claims.

## CLAIMS

1. A method of switching access for a mobile terminal between mobile networks, the mobile terminal comprising a first radio device capable of communication with a first mobile network and a second radio device capable of communication with a second mobile network, wherein the second mobile network has priority over the first mobile network, the method comprising the steps of:

- 5        - A) making an access request to the first mobile network by the mobile terminal using the first radio device,  
10      - B) authorising and establishing a first connection between the first radio device and the first mobile network,

15      **characterised by** the following further steps:

- C) detecting that the mobile terminal moves into a coverage area of the second mobile network,  
- D) authorising and establishing a second connection between the second radio device and the second mobile network based on the first authorising step B) for the first connection with the first mobile network.

20      2. A method according to claim 1, **characterised in** that the second authorising step D) includes exchanging authentication information between the first radio device and an authentication unit in the first mobile network, wherein the authentication information is used by the second radio device for accessing the second mobile network.

25

30      3. A method according to claim 2, **characterised in** that the exchanged authentication information comprises login

information according to a predetermined authentication agreement between the first and second mobile networks.

4. A method according to claim 3, **characterised in** that the exchanged information further comprises one or more encryption keys according to the predetermined authentication agreement.
5. A method according to claim 4, **characterised in** that payload data is communicated between the second radio device and the second mobile network in the connection authorised in step D), wherein the communicated payload data is protected by said exchanged encryption keys.
- 10 6. A method according to any of claims 1 - 5, **characterised in** that in the detecting step C), an identification signal, transmitted by the second mobile network, is detected by the second radio device.
- 15 7. A method according to any of claims 1 - 5, **characterised in** that in the detecting step C), an identification signal, transmitted by the second radio device, is detected by the second mobile network.
- 20 8. A method according to any of claims 1 - 5, **characterised in** that in the detecting step C), a locating function determines that the mobile device is located within the second network.
- 25 9. A method according to any of claims 1 - 8, **characterised in** that the first radio device is a mobile phone, the first mobile network is a GSM/GPRS network, the second

radio device is a PCCARD in a laptop computer being connected to the mobile phone, and the second mobile network is a WLAN.

- 5 10. A method according to any of claims 1 - 9, **characterised in** that the first mobile network covers a wide geographical area, and the second mobile network covers a limited overlapping spot area.
- 10 11. A mobile terminal comprising a first radio device capable of communication with a first mobile network and a second radio device capable of communication with a second mobile network, wherein the second mobile network has priority over the first mobile network, the first and a second radio devices are interconnected, and wherein the first radio device includes:
  - means for making an access request to the first mobile network, and
  - means for authorising and establishing a first connection with the first mobile network,**characterised in** that the first radio device further includes:
  - means for exchanging authentication information with an authentication unit in the first mobile network, when it is detected that the mobile terminal moves into a coverage area of the second mobile network, and that the second radio device further includes:
    - means for authorising and establishing a second connection with the second mobile network by using the exchanged authentication information.
- 15
- 20
- 25
- 30

12. A mobile terminal according to claim 11, **characterised in** that the first radio device further includes means for receiving login information according to a predetermined authentication agreement between the first and second  
5 mobile networks.

13. A mobile terminal according to claim 12, **characterised in** that the first radio device further includes means for receiving one or more encryption keys according to the  
10 predetermined authentication agreement.

14. A mobile terminal according to any of claims 11 - 13, **characterised in** that the second radio device comprises means for detecting an identification signal, transmitted  
15 by the second mobile network.

15. A mobile terminal according to any of claims 11 - 14, **characterised in** that the first radio device is a mobile phone capable of communication with a GSM/GPRS network,  
20 and wherein the second radio device is a PCCARD in a laptop computer, capable of communication with a WLAN.

16. An authentication unit for authenticating a mobile terminal comprising a first radio device capable of communication with a first mobile network and a second radio device capable of communication with a second mobile network, wherein the second mobile network has priority over the first mobile network, and wherein the authentication unit includes:  
25  
30 - means for authorising and establishing a first connection between the first radio device and the first mobile

network in response to an access request from the first radio device,

**characterised in** that the authentication unit further includes:

- 5 - means for exchanging authentication information with the first radio device when it is detected that the mobile terminal moves into a coverage area of the second mobile network, wherein the exchanged authentication information is used by the second radio device for accessing the  
10 second mobile network.

17. An authentication unit according to claim 16,

**characterised by** means for transmitting login information to the mobile terminal according to a predetermined  
15 authentication agreement between the first and second mobile networks.

18. An authentication unit according to claim 17,

**characterised by** means for transmitting one or more encryption keys to the mobile terminal according to the predetermined authentication agreement.  
20

19. An authentication unit according to any of claims 16 - 18, **characterised in** that the authentication unit belongs  
25 to the first mobile network.

20. An authentication unit according to claim 19,

**characterised in** that the authentication unit also belongs to the second mobile network.

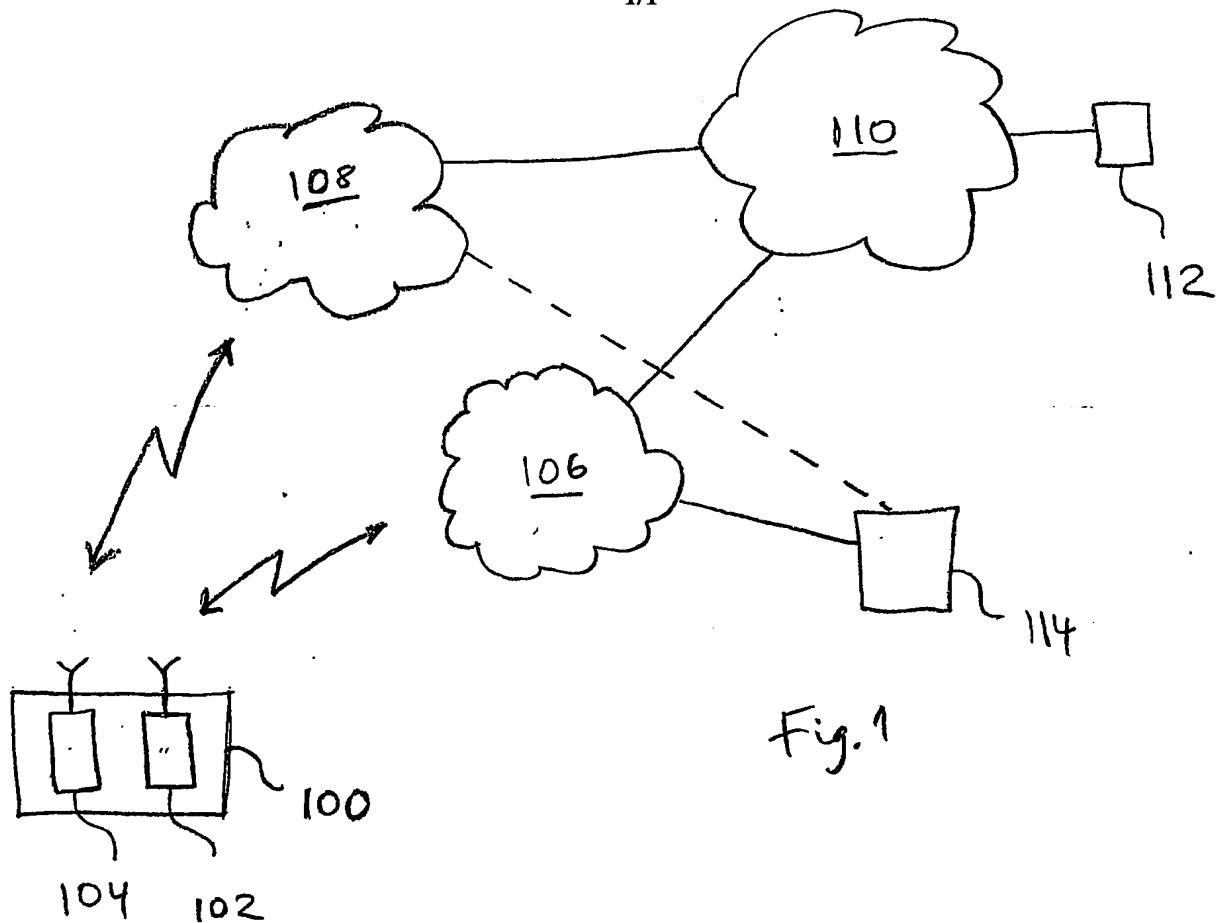


Fig. 1

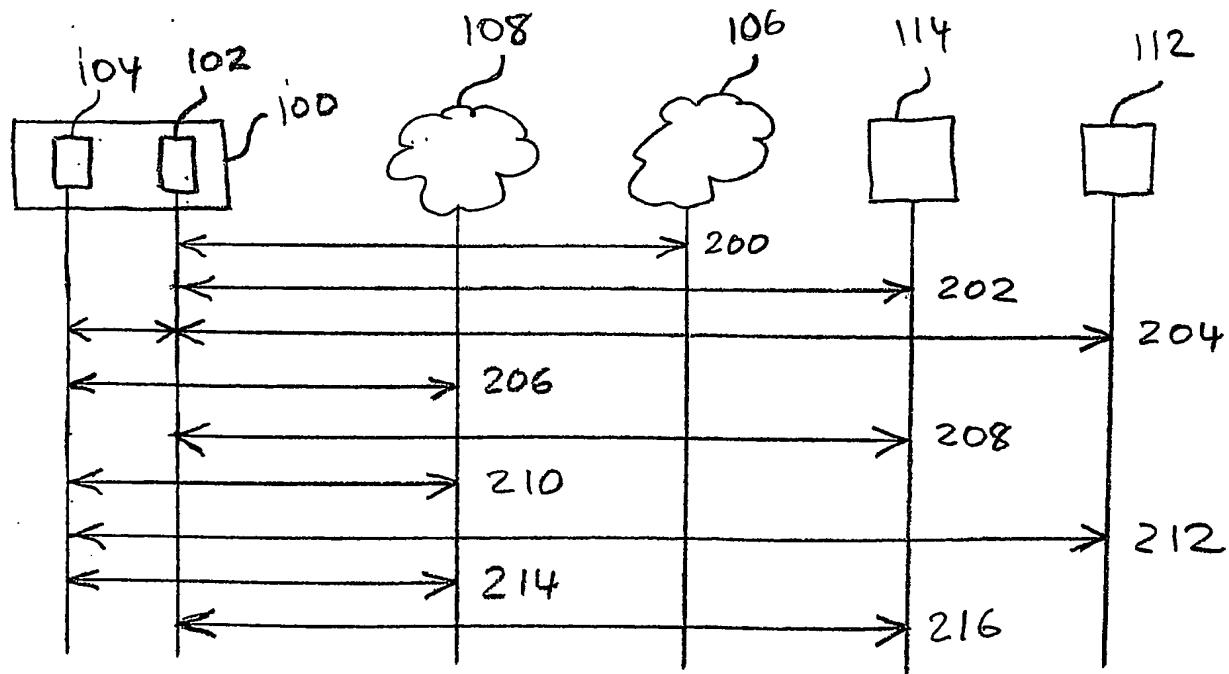


Fig. 2

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 02/02379

## A. CLASSIFICATION OF SUBJECT MATTER

**IPC7: H04Q 7/38**

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

**IPC7: H04Q**

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

**SE,DK,FI,NO classes as above**

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

**EPO-INTERNAL, WPI DATA, PAJ, INSPEC**

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 0158177 A2 (ORANGE PERSONAL COMMUNICATIONS SERVICES LIMITED), 9 August 2001 (09.08.01), page 2, line 9 - line 17; page 3, line 6 - line 22; page 4, line 11 - page 5, line 5, claims 1-14, abstract, page, line 21 - page 6, line 15 --	1-16
Y	WO 0041427 A3 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 13 July 2000 (13.07.00), page 1, line 18 - line 26; page 2, line 27 - page 3, line 2; page 9, line 10 - page 10, line 1, figure 2, abstract, claims 1-6,11-16,21-35 --	1-16
P,X	WO 02030132 A2 (NOKIA CORPORATION), 11 April 2002 (11.04.02), page 1 - page 3, abstract --	1-20

 Further documents are listed in the continuation of Box C. See patent family annex.

- \* Special categories of cited documents:
- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search

21 February 2003

Date of mailing of the international search report

13-03-2003

Name and mailing address of the ISA/  
Swedish Patent Office  
Box 5055, S-102 42 STOCKHOLM  
Facsimile No. +46 8 666 02 86Authorized officer  
  
Catharina Karlsson/mj  
Telephone No. +46 8 782 25 00

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 02/02379

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 0158190 A1 (TELIA AB), 9 August 2001 (09.08.01), page 4, line 15 - line 20; page 5, line 3 - page 6, line 25, figures 1,2, claims 1-24, abstract  -- -----	1,2,11,16

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

30/12/02

International application No.

PCT/SE 02/02379

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 0158177 A2	09/08/01	AU	3039601 A	14/08/01
		AU	5556400 A	31/01/01
		EP	1256254 A	13/11/02
		GB	0002495 D	00/00/00
		GB	0102567 D	00/00/00
		GB	2359220 A	15/08/01
		GB	2364620 A	30/01/02
		NO	20023664 A	11/09/02
-----	-----	-----	-----	-----
WO 0041427 A3	13/07/00	AU	2335300 A	24/07/00
		CN	1337134 T	20/02/02
		EP	1142400 A	10/10/01
		JP	2002534930 T	15/10/02
		US	6418130 B	09/07/02
-----	-----	-----	-----	-----
WO 02030132 A2	11/04/02	NONE		
-----	-----	-----	-----	-----
WO 0158190 A1	09/08/01	AU	3204800 A	14/09/00
		BR	0008400 A	29/01/02
		EP	1155503 A	21/11/01
		EP	1260109 A	27/11/02
		NO	20023519 A	02/10/02
		SE	0000335 A	03/08/01
-----	-----	-----	-----	-----